

**Password Policy**

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | Draft 25th June 2021 |
| Approved By | 5RB Management Committee |
| Effective Date | 25th June 2021 |
| Current Version | 1.1 |

Overview

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of 5RB's entire network, resulting in possible breach of confidentiality, heavy fines and adverse publicity. As such, all 5RB Barristers, staff & contractors (CTS & Lex) with access to systems are responsible for taking the appropriate steps, as outlined below to secure their passwords.

The UK GDPR does not say anything specific about passwords. However, Article 5(1)(f) states that personal data shall be:

*‘Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’*

This is the UK GDPR’s ‘integrity and confidentiality’ principle, or, more simply, the ‘security’ principle. So, although there are no provisions on passwords, the security principle requires you to take appropriate technical and organisational measures to prevent unauthorised processing of personal data you hold.

This means that when you are considering a password setup to protect access to a system that processes personal data, that setup must be ‘appropriate’.

Although the UK GDPR does not define what is ‘appropriate’, it does provide further considerations in Article 32, ‘security of processing’:

‘*Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.’*

This means that when considering any measures, you can consider the state of technological development and the cost of implementation – but the measures themselves must ensure a level of security appropriate to the nature of the data being protected and the harm that could be caused by unauthorised access.

In other words, you cannot simply set up a password system and then forget about it – there must be a periodic review process.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and importantly the frequency of change.

Scope

This policy applies to all 5RB barristers, staff and pupils that use information systems with user IDs and passwords. For example, accessing the network through a local computer, laptop, email or Lex software.

It applies whether using onsite 5RB Information Systems, Chambers laptops off site, or any privately owned devices, such as IPhones, IPads and laptops, used to access the above-mentioned systems.

Policy

This policy includes:

* The process of creating, changing and safeguarding passwords
* Policy and procedure to prevent the sharing of passwords with others
* Advice that users commit their passwords to memory and not allow them to be written or saved anywhere
* Policy and procedure governing the frequency of enforced password change

General

All user level passwords (email, desktop, laptop, Lex) must be changed on a regular basis and at least every 180 days.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user. E.g. the administrator password must be different to one used for a standard user account.

Passwords should never be inserted within e-mail messages or other forms of electronic communication. Nor must they be stored or transmitted in clear (unencrypted) text. Passwords should not be reused from other services.

All user-level and system-level passwords must confirm to the guidelines described below.

Guidelines

General requirements for any password system are password length, special characters and password deny lists. When selecting a password you should remember the stronger and longer the password, the more likely it will keep Information Systems and data secure:

* password length—this should be no less than 8 alphanumeric characters, (preferably 10 characters), it should also contain at least 3 out of 4 of the following:
	+ upper case character
	+ lower case character
	+ number
	+ special character

Passwords should preferably not include words found in the dictionary; it is good practice not to include words based on your personal information such as names of family members, pets etc.

Password Protection

Do not use the same password for 5RB accounts that you use for other non-5RB accounts, for example personal e-mail, online banking or social media.

Do not share 5RB passwords with anyone, including the clerks/admin team. All passwords are to be treated as confidential information.

Key points:

* Do not reveal a password over the phone to anyone
* Do not reveal a password in an email message
* Do not talk about a password in front of others
* Do not hint at the format of a password (e.g. family name)
* Do not reveal a password on questionnaires or security forms
* Take care when using social media so that you do not compromise your password
* Do not use the “remember password” feature (e.g. browsers, software applications)

Passwords must not be written down, nor should there be stored passwords in a file on ANY computer system or handheld device without encryption.

If an account or password is suspected to have been compromised, the incident must be reported to the Senior Clerk as soon as possible and the matter will be referred ASAP to CTS for assistance.

Changing your password and expiry

Guidance from the ICO advises that regular expiry often causes people to change a single strong password for a series of weak passwords.

It is agreed that passwords for 5RB systems will be changed every 180 days.

In the lead up to the date of expiry you will receive an email from Lex or the 5RB Administrator informing you that your password needs to be changed and you have ….

Either follow the link in the email **(be sure to check it is a valid email before clicking any link)** or go to <https://email.5rb.com/owa> and follow the procedure below: